

PROVING TOUCHARD'S THEOREM FROM EULER'S FORM

EYOB DELELE YIRDAW

ABSTRACT. This paper derives Touchard's theorem from Euler's form for odd perfect numbers. It also fine-tunes Euler's form.

A perfect number is a natural number N which satisfies $\sigma(N) = 2N$, where $\sigma(N)$ is defined as the sum of the divisors of N . Because $\sigma(ab) = \sigma(a)\sigma(b)$ when $\gcd(a, b) = 1$, $\sigma(N)$ is a multiplicative function. A handful of even perfect numbers are known and it is believed that infinite of them exist. It is also believed that odd perfect numbers do not exist. Euler showed that an odd perfect number N must be of the form $N = p^\alpha Q^2$ where p is a prime, $p \equiv \alpha \equiv 1 \pmod{4}$ and Q is an odd number such that $p \nmid Q$. Touchard [2] showed that $N = 12k + 1$ or $N = 36k + 9$. Euler's form manages to imply only $N \equiv 1 \pmod{4}$. We have to refine it a little bit to get to Touchard's theorem. Since p is prime, it can have only the form $12n + 1$ or $12n + 5$. Because α is always odd, $(p + 1) \mid \sigma(p^\alpha)$. Taking $p = 12n + 5$, we have $(12n + 6) \mid \sigma((12n + 5)^\alpha)$. Because $3 \mid (12n + 6)$, we have $3 \mid N$. Euler's form then becomes

$$(1) \quad N = (12n + 1)^\alpha Q^2 \quad \text{or} \quad N = (12n + 5)^\alpha (3Q)^2.$$

Using (1) we can prove Touchard's theorem. When $3 \mid N$, (1) becomes

$$N = p^\alpha (3Q)^2 = 9 \cdot p^\alpha Q^2 = 9(4k + 1) = 36k + 9.$$

When $3 \nmid N$, we use only $N = (12n + 1)^\alpha Q^2$, $3 \nmid Q$ (i.e., $Q \equiv 1 \pmod{6}$ or $Q \equiv 5 \pmod{6}$). Because $Q^2 \equiv 1 \pmod{12}$, $N = (12n + 1)^\alpha Q^2 \equiv 1 \pmod{12}$, completing the proof.

We can refine (1) a little bit further to

$$(2) \quad \begin{aligned} & N = (12n + 1)^{12\lambda+1} Q^2 \quad \text{or} \\ & N = (12n + 1)^{12\lambda+9} Q^2 \quad \text{or} \\ & N = (12n + 5)^{12\lambda+1} (3Q)^2 \quad \text{or} \\ & N = (12n + 5)^{12\lambda+9} (3Q)^2 \quad \text{or} \\ & N = (12n + 1)^{12\lambda+5} (3Q)^2 \quad \text{for } n \equiv 0, 1 \pmod{7} \quad \text{or} \\ & N = (12n + 5)^{12\lambda+5} (3Q)^2 \quad \text{for } n \equiv 2, 3 \pmod{7} \quad \text{or} \\ & N = (12n + 1)^{12\lambda+5} (21Q)^2 \quad \text{for } n \equiv 2, 3, 5, 6 \pmod{7} \quad \text{or} \\ & N = (12n + 5)^{12\lambda+5} (21Q)^2 \quad \text{for } n \equiv 0, 1, 4, 5 \pmod{7}. \end{aligned}$$

Date: March 18, 2008.

2000 Mathematics Subject Classification. Primary 11A25.

Key words and phrases. Odd perfect numbers, Touchard's theorem.

When $p = 12n + 1$ and $\alpha = 12\lambda + 5$,

$$(3) \quad \sigma((12n+1)^{12\lambda+5}) = [(12n+1)+1][(12n+1)^4 + (12n+1)^2 + 1] \sum_{\gamma=0}^{2\lambda} (12n+1)^{6\gamma}.$$

Here $3 \mid [(12n+1)^4 + (12n+1)^2 + 1]$. Thus $3 \mid N$ and (1) becomes $N = (12n+1)^{12\lambda+1}Q^2$ or $N = (12n+1)^{12\lambda+9}Q^2$ or $N = (12n+1)^{12\lambda+5}(3Q)^2$ or $N = (12n+5)^{4\lambda+1}(3Q)^2$. If n in (3) is congruent to 2, 3, 5 or 6 mod(7), then $7 \mid [(12n+1)^4 + (12n+1)^2 + 1]$ and hence $7 \mid N$. When $n \equiv 4 \pmod{7}$ p will not be prime. When $p = 12n + 5$ and $\alpha = 12\lambda + 5$, an argument similar to the above one gives $7 \mid N$ for $n \equiv 0, 1, 4, 5 \pmod{7}$.

Kuhnel's theorem [1] that $105 \nmid N$ requires $5 \nmid N$ in the last two forms of (2).

REFERENCES

1. Ullrich Khnel, *Verschrufung der notwendigen Bedingungen fr die Existenz von ungeraden vollkommenen Zahlen*, Mathematische Zeitschrift, vol. 52, 1949, pp. 201–211
2. J. Touchard, *On prime numbers and perfect numbers*, Scripta Math., vol. 19 , 1953, pp. 35–39.

ADDIS ABABA UNIVERSITY, ADDIS ABABA, ETHIOPIA
E-mail address: `edyirdaw@sis.aau.edu.et`